

AMENDMENTS TO THE DRAWINGS

A new set of formal drawings are included that have been amended in response to the issues raised by the Examiner. Each sheet is correctly identified as "Replacement Sheet".

REMARKS

Claims 1-18 are pending in the current application. In an Office Action dated December 19, 2006, the Examiner made six objections to the disclosure, objected to Figures 1A-C as failing to comply with 37 C.F.R. §1.84(p)(5), objected to Figure 3, objected to Figure 5, objected to claims 2, 5, 6, 10, and 14-17 for grammatical errors, rejected claims 5 and 14-15 under 35 U.S.C. §101, rejected claims 1-7 and 14-18 under 35 U.S.C. §102(e) as being anticipated by Wyatt, U.S. Patent No. 7,007,159 B2 ("Wyatt"), rejected claims 8-9 under 35 U.S.C. §103(a) as being unpatentable over Wyatt in view of Thomlinson et al., U.S. Patent No. 6,272,631 B1 ("Thomlinson"), and rejected claims 12-13 under 35 U.S.C. §103(a) as being unpatentable over Wyatt in view of Arbaugh et al., U.S. Patent No. 6,185,678 ("Arbaugh").

Applicant's representative respectfully asserts that the Examiner's objection to Figures 1A-C is not well founded. The Examiner states, in the objection, that Figures 1A-C "appear to be illustrating prior art." As clearly stated in the text of the current application, beginning on line 14 of page 1, as well as in the brief description of the drawings section, Figures 1A-C illustrate a secure-computing-platform booting problem as an example of the application of one embodiment of the present invention. In other words, the secure-computing-platform booting problem illustrated in Figures 1A-C is addressed by an embodiment of the present invention. Figures 1A-C do not illustrate any particular computer system or environment existing at the time that the application was filed and, as discussed in the background of the invention section of the current application, the techniques applied at the time of filing of the current application either involved complex, additional hardware, not shown in Figures 1A-C, or were not fully secure. Since Figures 1A-C are described as illustrating "a secure-computing-platform booting problem," do not show the additional hardware employed in certain of the previously existing techniques, and is described as being secure, Figures 1A-C cannot be honestly described as illustrating prior art.

The specification inadvertently included two erroneous numeric labels "1904" and "1902," as observed by the Examiner. The portion of the specification

including those erroneous numeric labels has been corrected, in the above amendment.

The Examiner also correctly noted an incorrect occurrence of the numeric label "312" on line 20 of page 10 of the current application. The specification is accordingly amended, in the above amendment.

The Examiner has correctly noted an ambiguity in the use of the numeric label "306" on line 19 of page 11. That numeric label should have directly followed the phrase "public encryption key 'PK2p\*.'" The portion of the specification including the improperly positioned numerical label "306" has been amended, in the above amendment.

The Examiner objected to inclusion of a reference to a web page in the current application. Finally, Applicant has amended the paragraph of the current application, in the above amendment, that included a reference to the web page <http://www.itl.nist.gov/fipspubs/fip180-1.htm>, to no longer refer to the web page.

As discussed above, Applicant's representative respectfully notes that Figures 1A-C cannot be labeled "prior art," as required by the Examiner in section 9 of the Office Action. These figures do not illustrate prior art.

With respect to the Examiner's objections in section 10 of the Office Action, the current specification correctly references numeric labels "202" and "204." With regard to the lack of an occurrence of the label "408," Applicant's representative has corrected the first paragraph on page 11 of the current application to include the numeric label "408."

With regard to the Examiner's objections stated in section 11 of the Office Action, Applicant's representative includes a corrected version of Figure 3. Similarly, with regard to the Examiner's objections stated in section 12 of the Office Action, Applicant's representative has included an amended Figure 5.

Finally, Applicant's representative has amended claims 2, 5, 6, 10, and 14-17 to address the Examiner's objections stated in section 15 of the Office Action. Thus, Applicant's representative believes that all claim and figure objections made by the Examiner, with the exception of the objection to Figures 1A-C, which Applicant's representative believes to be unfounded, have been addressed in the above amendments to the specifications and figures. Applicant's representative wishes to thank the Examiner

for the Examiner's careful attention to these numeric-label and figure-line deficiencies.

Applicant's representative respectfully traverses the Examiner's 35 U.S.C. §101 rejections of claims 5 and 14-15. In section 18 of the Office Action, the Examiner applies an incorrect test for patentability with regard to software conventions. Applicant's representative respectfully refers the Examiner to the USPTO's "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility." Claim 5, for example, claims computer instructions stored on a computer readable medium that implement the method of claim 1. Claim 1 claims a "method for preparing an authenticatable and verifiable image of a module," which, as described in the current application, is an important step for securely booting computer systems according to embodiments of the present invention. The subject matter of the method claim is entirely patentable, and therefore computer instructions that carry out the method, encoded on computer-readable medium, are also patentable. The computer-readable medium is a physical object that has been transformed to encode the instructions, and an authenticatable and verifiable image of a module, produced by such computer readable instructions when executed, is useful, concrete, and tangible. Moreover, the Examiner can find literally thousands of issued claims to computer instructions encoded in a computer-readable medium that carry out, or implement, useful methods.

With regard to the 35 U.S.C. §101 rejection of claim 15, the term "image" does not refer to a photograph or motion picture. The term "image" refers to executable code, stored in a computer-readable medium, as is well known to those familiar with software engineering, operating systems, and computer systems, in general. The Examiner can find many references to the term "image" throughout the current application, including references to "firmware image" on line 25 of page 2 and line 15 of page 3, and references to software module images on lines 11 and 14 of page 3. Furthermore, on line 22 of page 8, the term "executable image" can be found. A firmware-module image or software-module image is executable code that implements the firmware module or software module, respectively. Most telling, Wyatt also used the term "image" to refer to executable code, as, for example, on line 1 of column 13. Thus, the Examiner's rejection of claim 15 based on finding the term "image" to mean a

recorded photograph or motion picture, is simply in the clear context of the current application.

Applicant's representative respectfully traverses the Examiner's 35 U.S.C. §102 anticipation rejections of claims 1-7 and 14-18. The current application discloses a specific technique for preparing authenticatable and verifiable module images, as well as the authenticatable and verifiable firmware-module and software-module images themselves. An authenticatable and verifiable module image of a described embodiment of the present invention includes, as discussed beginning on line 17 of page 9 of the current application, and as clearly shown in Figure 3 of the current application, an ISLGUID header (302 in Figure 3) that includes an image size, location, and globally unique identifier ("GUID"). An authenticatable and verifiable module image of a described embodiment of the present invention additionally includes an authentication header (308 in Figure 3) that includes an encrypted, hashed module-specific public key (306 in Figure 3) and a clear-text version of that public key (308 in Figure 3). An authenticatable and verifiable module image of a described embodiment of the present invention additionally includes a digital signature (314 in Figure 3) obtained by hashing the contents of the firmware module (301 in Figure 3) and then encrypting the hashed value produced using a private encryption key (310 in Figure 3). These features of an authenticatable and verifiable image of the present invention are clearly claimed in independent claims 1, 6, 15, and 18. As an example, claim 1, provided below, is annotated with the numerical labels cited in the passage of the current application that describes Figure 3, beginning on line 17 of page 9 of the current application and extending to line 31 of page 10 of the current application:

1. (original) A method for preparing an authenticatable and verifiable image of a module, the method comprising:
  - receiving a module image;
  - adding to the module image (301) a size and location block (302);
  - adding to the module image an authentication block (308) including a cryptographically protected module-specific public key (306) and a clear-text version of the module-specific public key (308) to produce an authenticatable image; and

adding to the authenticable image a verification block (314) that includes a digital signature prepared from the module image.

Wyatt is essentially unrelated to the current application. Wyatt discloses a supplementary daughter-card (204 in Figure 2 of Wyatt) that is "used as an intermediary to flexibly augment the generic motherboard's display outputs and supply any display encoder needed to support the implemented display" (Wyatt, column 5, line 65 to column 6, line 1). In the current application, various hardware-implemented security appliances are discussed, beginning on line 20 of line 2, but are indicated in the Background of the Invention section of the current application as being inadequate because they require expensive engineering for incorporation into a secure computing environment. As can be appreciated from reading the current application, the methods disclosed and claimed in the current application do not rely on additional daughter cards or other such specific hardware devices.

The Examiner makes a number of specific references to Wyatt that the Examiner claims to teach various elements of the current claims. Applicant's representative specifically addresses recitations of Wyatt by the Examiner directed to the language of claim 1 as generally exemplary of the Examiner's 35 U.S.C. §102(e) rejections. For example, the Examiner points to line 39 of column 8, line 66 of column 8, and lines 39-45 of column 9 as teaching the second element of claim 1: "adding to the module image a size and location block." Line 39 of column 8 reads: "BIOS size thus appropriately appended. This allows the." This line does not refer to a value indicating the size of a module image stored within the module image, but instead appears to refer to an indication of the amount of memory currently used to store a shadow region. Line 66 of column 8 reads: "includes an example location/component for implementing." This disembodied portion of a larger sentence refers to a physical location or component within a hardware daughter card (204 in Figure 2 of Wyatt). Lines 39-45 of column 9 describe an exemplary arrangement of file systems which may be contained in a serially programmable device that is included in the hardware daughter card (204 in Figure 2 of Wyatt). Wyatt lists, in the cited passage, a number of headers and declarators within this file system, but does not teach, disclose, mention, or even suggest a "size and location

block." The two above-cited lines of column 8 do not refer to this file system discussed in lines 39-45 of column 9. Thus, the cited lines of Wyatt do not teach, mention, or suggest "adding to the module image a size and location block," are not related to one another, and are entirely unrelated to the subject matter to which claim 1 is directed.

With regard to the third element of claim 1, "adding to the module image and authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticatable image," the Examiner cites lines 63-64 of column 9, lines 14-15 of column 13, and lines 14-16 of column 13, and lines 17-25 of column 13. Lines 63-64 of column 9 read: "respect to the card 204 and/or devices 410, 420. Data block(s) 346' may contain data (e.g., tables, settings, param-"). This cited passage, and the enclosing sentences, do not teach, mention, or suggest any kind of authentication or support for authentication. Lines 14-15 of column 13 read: "erating a signature using the same algorithm, over the image, using the equivalent secret or public." These lines are part of a larger phrase describing a verification process in which a digital signature is apparently computed for a BIOS, and that signature is compared to a recomputed signature, both signatures obtained using a secret or public encryption key. Finally, lines 17-25 of column 13 of Wyatt reads:

If the result computed at run-time matches the stored signature value, it can assumed that the signature value retrieved from the image was authentic, and that the signature was produced by a trusted entity over a validated image (thereby verifying the "origin" of the image), and that the image has not been altered since validation had been performed (thereby verifying "integrity" of the image);

All of these cited portions of Wyatt, taken together, at most describe a very basic security method in which a digital signature is included in a BIOS, so that the digital signature can be recomputed, at a later time, to validate the contents of the BIOS. Wyatt does not teach, mention, or suggest including any kind of public key in a module, as claimed by the third element of claim 1, and does not teach, mention, disclose, or even suggest including an authentication block that contains a cryptographically protected module-specific public key and a clear-text version of that public key in a module. The cited portion of Wyatt is completely unrelated to the third element of claim 1.

The portions of Wyatt cited by the Examiner as teaching the third element of claim 1, which they do not, as discussed above, do, however, relate to the fourth element of claim 1, namely the verification block. Indeed, the Examiner cites portions of the paragraph spanning the end of column 12 and beginning on page 13 as teaching a verification block. While it is possible that these lines are related to the currently claimed "verification block," they are not in any way related to the claimed "authentication block."

The Examiner has thus failed to point to any teaching, mention, or disclosure of the second and third elements of claim 1 in Wyatt. Wyatt discloses a very simple, digital-signature-based authentication protocol, but not the validation and authentication method disclosed in the current application and claimed in the current claims. In particular, as noted above, applicant's method employs an authentication block including a hashed, encrypted public encryption key along with a clear-text version of the public-encryption key, that is included in verifiable and authenticable module images. Wyatt does not teach, mention, or suggest inclusion of such an authentication block, or any public key, whether in clear text or encrypted, in any firmware or software module. Claim 6 includes language directed to the authentication block claimed in claim 1, and claim 15 specifically claims an authentication block. Because Wyatt does not teach, mention, or suggest inclusion of an authentication block, an encrypted, hashed public key, or a clear-text public key in any software or firmware module, Wyatt cannot possibly anticipate the currently claimed invention. Because the independent claims are clearly not anticipated by Wyatt, the dependent claims of the current application are also not anticipated by Wyatt.

All of the 35 U.S.C. §103 rejections, including rejections of claims 8-9, 10-11, and 12 rely on a misinterpretation of Wyatt. For example, in the rejection of claims 8-9, the Examiner states: "Wyatt discloses the clear-text version of the module-specific public key (Col. 13, line 5); the hashed (Col. 12, line 65-67) encrypted module-specific public key (Col. 13, lines 14-15) and a first private encryption key (Col. 13, lines 1-2)." However, line 5 of column 13 reads: "original component vendor (for example Intel)," which obviously has nothing whatsoever to do with module-specific public keys.



Lines 65-67 of column 12 read: "such as SHA-1, MD5, cyclic redundancy check, (CRC) or other checksums, etc.) using digital signature techniques such as performing a one-way hash." Nothing in this portion of Wyatt discusses an encrypted module-specific public key. Instead, this portion of Wyatt discusses a variety of different hashing algorithms that, in the first line of column 13 of Wyatt, are described as functioning over the image, rather than as being applied to a module-specific public key, as claimed in the current claims. Lines 14-15 of column 13, as previously discussed, are related to computing a digital signature over an image, and have nothing whatsoever to do with encrypting or hashing a module-specific public key. Because of the clear misinterpretation of the teachings of Wyatt, and the reliance on the teachings of Wyatt for rejection of claims 8-9 by the Examiner, the Examiner's 35 U.S.C. §103(a) rejections of claims 8-9 are unfounded.

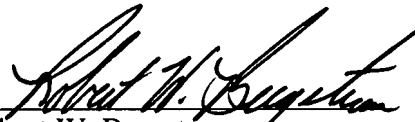
Similar reasoning applies to the rejections of claims 10 and 11 under 35 U.S.C. §103(a). Wyatt, as discussed above, does not disclose a "size and location block," and also does not teach, mention, or suggest a "module-specific public key." Thus, the rejection of claims 10-11 under 35 U.S.C. §103(a), relying on a misinterpretation of Wyatt, is unfounded. Similarly, the Examiner relies on Wyatt, in the rejection of claims 12-13, but, as discussed above, these claims depend from claim 6, which explicitly cites extraction of a "module-specific public key and cryptographically protected data related to the module-specific public key" from an "authenticatable and verifiable module." Wyatt does not teach, mention, or suggest a module-specific public key and cryptographically protected data related to the module-specific public key being incorporated into an authenticatable or verifiable module. Again, the rejection of claims 12-13 under 35 U.S.C. §103(a) is based, in part, on a misinterpretation of Wyatt, and is therefore unfounded.

In summary, the current application is directed to a specific secure-boot method involving authenticatable and verifiable modules that include, in addition to a digital signature, an authentication block and an ISLGUID header, referred to in the current claims as "a size and location block." Wyatt does not teach, mention, or suggest the disclosed and claimed authentication block, inclusion of any kind of public key or

cryptographically protected public key within a software or firmware module. Because all of the claim rejections are based on Wyatt teaching an authentication block, which Wyatt neither teaches, mentions, or even suggests, all the claim rejections are unfounded.

In Applicant's representative's opinion, all of the claims remaining in the current application are clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,  
Chris D. Hyser  
Olympic Patent Works PLLC

  
Robert W. Bergstrom  
Registration No. 39,906

Enclosures:

Postcards(2)  
Transmittal in duplicate  
Extension of Time in duplicate

Olympic Patent Works PLLC  
P.O. Box 4277  
Seattle, WA 98194-0277  
206.621.1933 telephone  
206.621.5302 fax